Aniket Kate

Department of Computer Science
Purdue University
https://www.cs.purdue.edu/homes/akate/
aniket@purdue.edu

305 N. University Street
West Lafayette, IN 47907
USA 47907
Office: +1-765-496-2763

Date: *October 31, 2020*

EDUCATION

Ph.D., Computer Science, University of Waterloo, Canada, 2010
Advisor: Ian Goldberg

M.Tech., Computer Science and Engineering, Indian Institute of Technology–Bombay, India, 2006

B.E., Information Technology, Mumbai University, India, 2003

RESEARCH INTEREST

I am an applied cryptographer and a privacy researcher. My research builds on and expands applied cryptography, distributed computing, and data-driven analysis toward developing and analyzing robust solutions for privacy and (distributed) trust. My current research projects focuses on communication freedom and distributed ledger (or blockchain) protocols.
In my group, (i) we design and analyze efficient, provably secure cryptographic solutions for anonymous communication, and formalize and realize privacy and censorship-resistance for the emerging communication modalities over the Internet; (ii) we enhance security, privacy, and reliability of distributed ledgers and communication across dissimilar ledgers, and devise their novel crypto-economic applications to the financial world, supply chains and beyond.

EXPERIENCE

Computer Science, Purdue University — West Lafayette, IN, USA
Associate Professor — Aug 2020–*present*

Computer Science, Purdue University — West Lafayette, IN, USA
Assistant Professor — Aug 2015–*Aug 2020*

Cluster of Excellence, Saarland University — Saarbruecken, Germany
Junior Faculty Member, Independent Research Group Leader — Aug 2012–Sep 2015

Max Planck Institute for Software Systems (MPI-SWS) — Saarbruecken, Germany
Postdoctoral Researcher with Michael Backes — Sep 2010–July 2012

University of Waterloo — Waterloo, Canada
Research Assistant with Ian Goldberg — May 2007–Aug 2010
Research Assistant with Urs Hengartner — Sep 2006–Apr 2007

AWARDS AND HONORS

INTERNAL TO PURDUE

- ◇ Purdue Seed for Success award, 2019.
- ◇ College of Science Faculty Team Award, February 2016.

EXTERNAL TO PURDUE

- ◇ National Science Foundation (NSF) CAREER Award, February 2019.
- ◇ Cyber Security Awareness Week (CSAW) Applied Research Award (Top-10) Finalist, November 2017.
- ◇ Best paper award at ACM Conference on Online Social Networks (COSN), November 2015.
- ◇ David R. Cheriton Graduate Scholarship, University of Waterloo, 2007–2010.

REFEREED PUBLICATIONS

Note: * indicates primary author, ^{P} denotes author who is postdoctoral researcher (or on other pre-faculty position) *at the time of writing*. ^{U} and ^{G} similarly indicate authors who were undergraduate and graduate students respectively *at the time of writing*. Publications with previous mentors are distinguished by the ^{M} tag.

JOURNAL ARTICLES

[Post-Purdue Hire]

1 Debajyoti Das^{*G}, Sebastian Meiser, Esfandiar Mohammadi, and Aniket Kate. Comprehensive Anonymity Trilemma: User Coordination is not enough. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2020(3), 356–383, 2020.

2 Mohsen Minaei^{*G}, Pedro Moreno-Sanchez^{*G}, and Aniket Kate. MoneyMorph: Censorship Resistant Rendezvous using Permissionless Cryptocurrencies. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2020(1), 404–424, 2020.

3 Duc Le^{*G}, Lizzy Tengana Hurtado^U, Adil Ahmad, Mohsen Minaei^G, Byoungyoung Lee, and Aniket Kate. A Tale of Two Trees: One Writes, and Other Reads. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2020(2), 519–536, 2020.

4 Mohsen Minaei^{*G}, Mainack Mondal^P, Patrick Loiseau, Krishna Gummadi, and Aniket Kate. Lethe: Conceal Content Deletion from Persistent Observers. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2019(1), 206–226, 2019.

5 Pedro Moreno-Sanchez^{*G}, Uzair Mahmood^G, and Aniket Kate. ClearChart: Ensuring Integrity of Consumer Ratings in Online Marketplaces. *Computers & Security Journal (CoSe)*, 78: 90–102, 2018.

6 Pedro Moreno-Sanchez^{*G}, Tim Ruffing^G, and Aniket Kate. PathShuffle: Credit Mixing and Anonymous Payments for Ripple. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2017 (3), 2017.

7 Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi. AnoA: A Framework for Analyzing Anonymous Communication Protocols. *Journal of Privacy and Confidentiality (JPC)*, 7(2): 79–125, 2016.

8 Pedro Moreno-Sanchez*, Muhammad Bilal Zafar^G, and Aniket Kate. Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network. *Proceedings on Privacy Enhancing Technologies (PoPETS)*, Vol. 2016(4), 2016.

9 Michael Backes, Niklas Grimm^{*U}, and Aniket Kate. Data Lineage in Malicious Environments. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 13(2): 178-191, 2016.
[Pre-Purdue Hire]

10 Maxwell Young*, Aniket Kate, Ian Goldberg, and Martin Karsten. Towards Practical Communication in Byzantine-Resistant DHTs.^{M} *IEEE/ACM Transactions on Networking (ToN)*, 21(1), 2013.

11 Aniket Kate*and Ian Goldberg. Generalizing Cryptosystems Based on the Subset Sum Problem.^{M} *Springer International Journal of Information Security (IJIS)*, 10 (3), 2011.

12 Aniket Kate*, Gregory M. Zaverucha, and Ian Goldberg. Pairing-Based Onion Routing with Improved Forward Secrecy.^{M} *ACM Transactions on Information and System Security (TISSEC), 13(4)*, 2010.

CONFERENCE PUBLICATIONS

[Post-Purdue Hire]

13 Mohsen Minaei^{*G}, S Chandra Mouli, Mainack Mondal, Bruno Ribeiro, and Aniket Kate. Cloaking Large-Scale Damaging Deletions on Social Platforms. *To appear at* Network and Distributed System Security Symposium (NDSS), Feb 2021.

14 Sri Aravinda Krishnan Thyagarajan^{*G}, Adithya Bhat^G, Giulio Malavolta, Nico Doettling, Aniket Kate, and Dominique Schroeder Verifiable Timed Signatures Made Practical. *To appear at* 27th ACM Conference on Computer and Communications Security (CCS), Nov 2020.

15 Venkat Arun^{*U}, Aniket Kate, Deepak Garg, Peter Druschel, and Bobby Bhattacharjee. Finding Safety in Numbers with Secure Allegation Escrows. Network and Distributed System Security Symposium (NDSS), Feb 2020. (17% acceptance rate)

16 Pedro Moreno-Sanchez*, Randomrun, Duc Le^{G}, Sarang Noether, Brandon Goodell and Aniket Kate. DLSAG: Non-Interactive Refund Transactions For Interoperable Payment Channels in Monero. 24th International Conference on Financial Cryptography and Data Security (FC), Feb 2020. (22% acceptance rate)

17 Donghang Lu*^{G}, Tom Yurek, Samarth Kulshreshtha, Rahul Mahadev, Aniket Kate, and Andrew Miller. HoneyBadgerMPC and AsynchroMix: Practical Asynchronous MPC and its Application to Anonymous Communication. 26th ACM Conference on Computer and Communications Security (CCS), Nov 2019. (16% acceptance rate)

18 Duc V. Le*^{G}, Mahimna Kelkar^{U}, and Aniket Kate. Flexible Signatures: Towards Making Authentication Suitable for Real-Time Environments. European Symposium on Research in Computer Security (ESORICS), Sep 2019. (19% acceptance rate)

19 Michael Backes, Lucjan Hanzlik, Amir Herzberg, Aniket Kate, and Ivan Pryvalov*. Efficient Non-Interactive Zero-Knowledge Proofs in Cross-Domains without Trusted Setup. 22nd International Conference on Practice and Theory of Public Key Cryptography (PKC), Apr 2019. (24% acceptance rate)

20 Giulio Malavolta*, Pedro Moreno-Sanchez*^{G}, Clara Schneidewind, Aniket Kate, Matteo Maffei. Anonymous Multi-hop Locks for Blockchain Scalability and Interoperability. Network and Distributed System Security Symposium (NDSS), Feb 2019 (17% acceptance rate)

21 Sze Yiu Chau*^{G}, Moosa Yahyazadeh, Omar Chowdhury, Aniket Kate, and Ninghui Li. Analyzing Semantic Correctness using Symbolic Execution: A Case Study on PKCS#1 v1.5 Signature Verification Network and Distributed System Security Symposium (NDSS), Feb 2019 (17% acceptance rate)

22 Sze Yiu Chau*^{G}, Bincheng Wang, Jianxiong Wang, Omar Chowdhury, Aniket Kate, and Ninghui Li. Why Johnny Can't Make Money With His Contents: Pitfalls of Designing and Implementing Content Delivery Apps. Annual Computer Security Applications Conference (ACSAC), pp. 236-251, December 2018. (20% acceptance rate)

23 Debajyoti Das*^{G}, Sebastian Meiser, Esfandiar Mohammadi, and Aniket Kate. Anonymity Trilemma: Strong Anonymity, Low Bandwidth, Low Latency—Choose Two. 39th IEEE Symposium on Security and Privacy (S&P (Oakland)), May 2018. (11% acceptance rate)

24 Pedro Moreno-Sanchez*^{G}, Navin Modi, Raghuvir Songhela, Aniket Kate, and Sonia Fahmy. Mind Your Credit: Assessing the Health of the Ripple Credit Network. 27th World Wide Web Conference (WWW), April 2018. (15% acceptance rate)

25 Stefanie Roos*, Pedro Moreno-Sanchez^{G}, Aniket Kate, and Ian Goldberg. Settling Payments Fast and Private: Efficient Decentralized Routing for Path-Based Transactions.^{M} Network and Distributed System Security Symposium (NDSS), Feb 2018. (21% acceptance rate)

26 Giulio Malavolta*, Pedro Moreno-Sanchez*^{G}, Aniket Kate, Matteo Maffei, and Srivatsan Ravi^{P}. Concurrency and Privacy with Payment-Channel Networks. 24th ACM Conference on Computer and Communications Security (CCS), Oct 2017 (18% acceptance rate)

27 David Chaum, Debajyoti Das^{G}, Farid Javani, Aniket Kate, Anna Krasnova, Joeri de Ruiter, & Alan T. Sherman. cMix: Mixing with Minimal Real-Time Asymmetric Cryptographic Operations. 15th International Conference on Applied Cryptography and Network Security (ACNS), Jun 2017 (23% acceptance rate)

28 Sze Yiu Chau*^{G}, Endadul Hoque, Omar Chowdhury, Huangyi Ge, Aniket Kate, Cristina Nita-Rotaru, and Ninghui Li. Systematically Finding Non-compliances In X.509 Certificate Validation Implementations. 38th IEEE Symposium on Security and Privacy (Oakland), May 2017 (13% acceptance rate)

29 Tim Ruffing*^{G}, Pedro Moreno-Sanchez^{G}, and Aniket Kate. P2P Mixing and Unlinkable Bitcoin Transactions. Network & Distributed System Security Symposium (NDSS), Feb 2017 (16% acceptance rate)

30 Giulio Malavolta*, Pedro Moreno-Sanchez*^{G}, Aniket Kate, and Matteo Maffei. SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks. Network and Distributed System Security Symposium (NDSS), Feb 2017 (16% acceptance rate)

31 Michael Backes, Amir Herzberg, Aniket Kate, and Ivan Pryvalov*. Anonymous RAM. 21st European Symposium on Research in Computer Security (ESORICS), Sep 2016 (21% acceptance rate)

32 Mainack Mondal*, Johnnatan Messias, Saptarshi Ghosh, Krishna P. Gummadi, and Aniket Kate. Forgetting in Social Media: Understanding and Controlling Longitudinal Exposure of Socially Shared Data. USENIX Symposium on Usable Privacy and Security (SOUPS), Jun 2016 (28% acceptance rate)

33 Bimal Viswanath*, Muhammad Ahmad Bashir, Muhammad Bilal Zafar, Simon Bouget, Saikat Guha, Krishna P. Gummadi, Aniket Kate, and Alan Mislove. Strength in Numbers: Robust Tamper Detection in Crowd Computations. ACM Conference on Online Social Networks (COSN), Nov 2015 (27% acceptance rate)

34 Tim Ruffing*^{G}, Aniket Kate, and Dominique Schroeder. Liar, Liar, Coins on Fire!: Penalizing Equivocation By Loss of Bitcoins. 22nd ACM Conference on Computer and Communications Security (CCS), Oct 2015 (20% acceptance rate)

[Pre-Purdue Hire]

35 Satrajit Ghosh^{G}and Aniket Kate*. Post-Quantum Forward Secure Onion Routing (Future Anonymity in Today's Budget). 13th International Conference on Applied Cryptography and Network Security (ACNS), Jun 2015 (21% acceptance rate)

36 Michael Backes, Aniket Kate, Sebastian Meiser*, and Tim Ruffing^{G}. Secrecy without Perfect Randomness: Cryptography with (Bounded) Weak Sources. 13th International Conference on Applied Cryptography and Network Security (ACNS), Jun 2015 (21% acceptance rate)

37 Daniel Porto*, Joao Leitao, Cheng Li, Allen Clement, Aniket Kate, Flavio Junqueira, and Rodrigo Rodrigues. Visigoth Fault Tolerance. European Conference on Computer Systems (EuroSys), Apr 2015 (21% acceptance rate)

38 Pedro Moreno-Sanchez*^{G}, Aniket Kate, Matteo Maffei, and Kim Pecina. Privacy Preserving Payments in Credit Networks. Network and Distributed System Security Symposium (NDSS), Feb 2015 (17% acceptance rate)

39 Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov^{G}. Privacy-preserving Data Aggregation with Optimal Utility. 30th Annual Computer Security Applications Conference (ACSAC), Dec 2014 (20% acceptance rate)

40 Michael Backes, Aniket Kate, Sebastian Meiser*, and Esfandiar Mohammadi. (Nothing else) MATor(s): Monitoring the Anonymity of Tor's Path Selection. 21st ACM Conference on Computer and Communications Security (CCS), Nov 2014 (19% acceptance rate)

41 Tim Ruffing*^{G}, Pedro Moreno-Sanchez^{G}, and Aniket Kate. CoinShuffle: Practical Decrentralized Coin Mixing for Bitcoin. 19th European Symposium on Research in Computer Security (ESORICS), Sep 2014 (25% acceptance rate)

42 Michael Backes, Fabian Bendun, Ashish Choudhury, and Aniket Kate*. Asynchronous MPC with a Strict Honest Majority Using Non-equivocation. 33rd ACM Symposium on Principles of Distributed Computing (PODC), Jul 2014 (28% acceptance rate)

43 Michael Backes, Jeremy Clark, Peter Druschel, Aniket Kate, and Milivoj Simeonovski*. Introducing Accountability to Anonymity Networks. 12th International Conference on Applied Cryptography and Network Security (ACNS), Jun 2014 (22% acceptance rate)

44 Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi. AnoA: A Framework For Analyzing Anonymous Communication Protocols. 26th IEEE Computer Security Foundations Symposium (CSF), Jun 2013 (26% acceptance rate)

45 Michael Backes, Amit Datta^{U}, and Aniket Kate*. Asynchronous Computational VSS with Reduced Communication Complexity. Cryptographers' Track - RSA Conference (CT-RSA), Feb 2013 (28% acceptance rate)

46 Allen Clement, Flavio Junqueira, Aniket Kate*, and Rodrigo Rodrigues. On the (Limited) Power of Non-Equivocation. 31st ACM Symposium on Principles of Distributed Computing (PODC), Jul 2012 (26% acceptance rate)

47 Michael Backes, Ian Goldberg, Aniket Kate, and Esfandiar Mohammadi*. Provably Secure and Practical Onion Routing.^{M} 25th IEEE Computer Security Foundations Symposium (CSF), Jun 2012 (25% acceptance rate)

48 Michael Backes, Aniket Kate*, Matteo Maffei, and Kim Pecina. ObliviAd: Provably Secure and Practical Online Behavioral Advertising. 33rd IEEE Symposium on Security and Privacy (Oakland), May 2012 (13% acceptance rate)

49 Michael Backes, Ian Goldberg, Aniket Kate*, and Tomas Toft. Adding Query Privacy to Robust DHTs.^{M} 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS), May 2012 (22% acceptance rate)

50 Michael Backes, Aniket Kate, and Arpita Patra. Computational Verifiable Secret Sharing Revisited. 17th International Conference on the Theory and Application of Cryptology (ASIACRYPT), Dec 2011 (15% acceptance rate)

51 Aniket Kate*, Gregory M. Zaverucha, and Ian Goldberg. Constant-Size Commitments to Polynomials and Their Applications.^{M} 16th International Conference on the Theory and Application of Cryptology (ASIACRYPT), Dec 2010 (16% acceptance rate)

52 Aniket Kate*and Ian Goldberg. Distributed Private-Key Generators for Identity-Based Cryptography.^{M} 7th Conference on Security and Cryptography for Networks (SCN), Sep 2010 (28% acceptance rate)

53 Maxwell Young*, Aniket Kate, Ian Goldberg, and Martin Karsten. Practical Robust Communication in DHTs Tolerating a Byzantine Adversary.^{M} 30th International Conference on Distributed Computing Systems (ICDCS), Jun 2010 (14% acceptance rate)

54 Aniket Kate*and Ian Goldberg. Using Sphinx to Improve Onion Routing Circuit Construction.^{M} 14th International Conference on Financial Cryptography & Data Security (FC), Jan 2010 (19% acceptance rate)

55 Aniket Kate*and Ian Goldberg. Distributed Key Generation for the Internet.^{M} 29th International Conference on Distributed Computing Systems (ICDCS), Jun 2009 (16% acceptance rate)

56 Aniket Kate*, Gregory M. Zaverucha, and Urs Hengartner. Anonymity and Security in Delay Tolerant Networks. 3rd International Conf. on Security and Privacy in Communication Networks (SecureComm), Sep 2007 (26% acceptance rate)

57 Aniket Kate*, Gregory M. Zaverucha, and Ian Goldberg. Pairing-Based Onion Routing.^{M} 7th Privacy Enhancing Technologies Symposium (PET), Jun 2007 (19% acceptance rate).

REFEREED MAGAZINE ARTICLES

[Post-Purdue Hire]

58 Ryan Henry, Amir Herzberg, and Aniket Kate. Blockchain Access Privacy: Challenges and Directions. IEEE Security and Privacy Magazine, July/August 2018.

59 Mainack Mondal*, Johnnatan Messias, Saptarshi Ghosh, Krishna P. Gummadi, and Aniket Kate. Longitudinal Privacy Management in Social Media: The Need for Better Controls. IEEE Internet Computing (IC), 21(3), 2017.

REFEREED WORKSHOP PAPERS

[Post-Purdue Hire]

60 Easwar V Mangipudi*^{G}, Krutarth R Rao^{U}, Jeremy Clark, and Aniket Kate. Towards Automatically Penalizing Multimedia Breaches. IEEE Security & Privacy on the Blockchain (IEEE S&B) Workshop, Jun 2019.

61 Donghang Lu*^{G}, Pedro Moreno-Sanchez^{G}, Amanuel Zeryihun, Shivam Bajpayi^{U}, Sihao Yin^{U}, Ken Feldman, Jason Kosofsky, Pramita Mitra, and Aniket Kate. Reducing Automotive Counterfeiting using Blockchain: Benefits and Challenges. IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Apr 2019.

62 Adithya Bhat*^{G}, Pedro Moreno-Sanchez and Aniket Kate. Transitive Network: Tokenless IOU Credit Network in Ethereum. Cryptocurrency Implementers' Workshop (CIW), co-located with FC 2019, Feb 2019.

[Pre-Purdue Hire]

63 Michael Backes, Niklas Grimm*^{U}, and Aniket Kate. Lime: Data Lineage in the Malicious Environment. 10th International Workshop on Security and Trust Management (STM), Sep 2014.

64 Tim Ruffing*^{G}, Jonas Schneider, Aniket Kate. Identity-Based Steganography and Its Applications to Censorship Resistance. 6th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), Jul 2013.

65 Michael Backes, Aniket Kate, and Esfandiar Mohammadi*. Ace: An Efficient Key-Exchange Protocol for Onion Routing. 11th ACM Workshop on Privacy in the Electronic Society (WPES), Oct 2012.

BOOKS AND BOOK CHAPTERS

66 Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov^{G}. Achieving Optimal Utility for Distributed Differential Privacy Using Secure Multiparty Computation. Book chapter, "Applications of Secure Multiparty Computation", IOS CISS, 13(5), 2015

67 Aniket Kate, Matteo Maffei, Giulio Malavolta, and Pedro Moreno-Sanchez^{G}. Credit Networks: Decentralized Designs and Privacy. To appear in *Morgan & Claypool's Information Security, Privacy, and Trust series*, pgs. 130, 2019

POSTERS

68 Tim Ruffing^{*G}, Jonas Schneider, Aniket Kate. Poster: Identity-based steganography and its applications to censorship resistance. ACM Conference on Computer and Communications Security (CCS), Oct 2013

69 Michael Backes, Fabian Bendun, and Aniket Kate*. Brief Announcement: Distributed Cryptography using TrInc. 31$^{\text{st}}$ ACM Symposium on Principles of Distributed Computing (PODC), Jul 2012

THESES

70 Aniket Pundlik Kate: "Distributed Key Generation and Its Applications"
PhD Thesis, University of Waterloo, Jun 2010

71 Aniket Kate: "Frobenius Endomorphism Based Cryptosystems"
Master Thesis, Indian Institute of Technology–Bombay, Jun 2006

TECHNICAL REPORTS

72 Sanjit Chatterjee, Deepak Garg, Aniket Kate*, and Tobias Theobald^{G}. Encrypting Messages for Incomplete Webs of Trust. IACR Cryptology ePrint Archive 2017: 777, August 2017.

73 Ivan Pryvalov^{*G}, Aniket Kate. Introducing Fault Tolerance into Threshold Password-Authenticated Key Exchange. IACR Cryptology ePrint Archive 2014: 247, July 2014.

74 Aniket Kate*, Yizhou Huang, and Ian Goldberg. Distributed Key Generation in the Wild.^{M} IACR Cryptology ePrint Archive 2012/377, Jul 2012.

SELECTED INVITED TALKS

NATIONAL AND INTERNATIONAL MEETINGS

- "Blockchains + Network Privacy = A Nightmare," The 2020 Information Theory and Applications Workshop, San Diego. Feb 2020.
- "Anonymous multi-hop locks for Blockchain scalability and interoperability," Cryptoeconomic Systems Summit at the MIT Media Lab. Oct 2019.
- "Next Frontiers in Blockchains: Privacy and Interoperability," Blockchain and Other Networks Conference, TTI/Vanguard, Washington, D.C. Sep 2019.
- "Blockchain Scalability and Interoperability," Workshop on Security of Permissionless Systems (SPS), co-located with ACM PODC 2019. Aug 2019.
- **Keynote**: "Building Decentralized Credit Networks" at the Blockchain Connect Conference, San Francisco. Jan 2019.
- "Blockchain Contracts + Cryptography = Decentralized Economy!?" at the Workshop on Competitive Economics of Cybersecurity, Sandia National Laboratories. Nov 2018.
- Invited Speaker: "Inventing and Re-Inventing Blockchains for Supply-chain and IoT" at the 5th annual Indy Big Data Conferences. Sept 2018
- "Blockchain Privacy: Challenges, Solutions, and Unresolved Issues" at Blockchain and Cryptocurrency Workshop, Calgary, Canada. Aug 2017.
- **Keynote**: "Distributed IOweYou Credit Networks" at 18th International Conference on Distributed Computing and Networking (ICDCN), Hyderabad, India. Jan 2017.
- Tutorial: "An Introduction to Credit Networks" at ACM Conference on Computer and Communications Security (CCS), Vienna, Austria. Oct 2016.

- ◇ "Distributed IOweYou Credit Networks" at Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016), co-located with PODC 2016. July 2016.
- ◇ "(Working group) Genome Privacy: Architecture and middleware" at Dagstuhl Seminar 15431, Dagstuhl, Germany. Oct 2015.
- ◇ "Future Anonymity in Today's Budget" at NIST Workshop on Cybersecurity in a Post-Quantum World (NIST PQC), Gaithersburg, USA. Apr 2015.
- ◇ "Asynchronous MPC with a Strict Honest Majority Using Non-equivocation" at Applied Multi-Party Computation Workshop, Microsoft Research, Redmond, USA. Feb 2014.
- ◇ "Anonymous Key Agreement in an Identity-based Infrastructure and its Applications" at the *MITACS 2009 Annual Conference*, Canada. Jun 2009.

UNIVERSITIES AND OTHER INSTITUTIONS

- ◇ Four lectures on "Blockchains and Cryptocurreices" at UNAM/ITAM, Mexico City, Mar 2019.
- ◇ "Towards Inter-blockchain Communications", Systems Seminar Speaker, Cornell University, Oct 2018.
- ◇ "Blockchains for (Digital) Supply Chains and Beyond", Invited Speaker Series, SRC Inc, Syracuse, Oct 2018.
- ◇ "Blockchain Privacy : Challenges and Solutions" at the Workshop on Blockchain Technology, R C Bose Centre for Cryptology, Kolkata, India. Nov 2017. (Virtual Seminar)
- ◇ "Distributed IOweYou Credit Networks" at Visa Research, Palo Alto. Nov 2017.
- ◇ "Blockchain Privacy: Challenges, Solutions, and Unresolved Issues" at Cylab Distinguished Seminar Series, CMU. Oct 2017.
- ◇ Tutorial: "IOweYou Credit Networks" at 2nd Hebrew University Networking Summer, Jerusalem, Israel. Jun 2017.
- ◇ "IOweYou Credit Networks" at Information Trust Institute, University of Illinois at Urbana-Champaign, Mar 2017.
- ◇ "IOweYou Credit Networks" at CS, University of Wisconsin-Madison, Feb 2017.
- ◇ "Enabling trust with privacy in virtual marketplaces using credit networks" at Computer Science (CS) Colloquium Series, Indiana University, Bloomington. Apr 2016.
- ◇ "A little trusted hardware can go a long way towards privacy" at CASED, TU Darmstadt, Germany. Mar 2015.
- ◇ "Anonymous Communication Networks: Design, Analysis and Challenges" at TU Dresden, Germany. Sep 2014.
- ◇ "Differential Guarantees for Cryptographic Systems" at Microsoft Research, India. Apr 2014.
- ◇ "Towards Practical and Efficient Distributed Trust" at Indian Institute of Technology—Kharagpur (IIT-Kgp), India. Sep 2012.
- ◇ "An Interplay between Anonymity, Privacy, and Accountability" at *Indian Statistical Institute (ISI)*, India. Sep 2012.
- ◇ "Recent Improvements to Onion Routing" at *IBM Research - Zurich*, Rueschlikon, Switzerland. Jan 2012.
- ◇ "Recent Improvements in Onion Routing Circuit Construction" in the *Laboratory of Algorithmics, Cryptology and Security (LACS), University of Luxembourg*, Luxembourg. Feb 2010.

OTHER PRESENTED PAPERS

- ◇ "Post-Quantum Forward-Secure Onion Routing - (Future Anonymity in Today's Budget)," ACNS 2015, New York, Jun 2015.
- ◇ "Asynchronous MPC with a strict honest majority using non-equivocation," ACM PODC 2014, Paris, July 2014.
- ◇ "Asynchronous Computational VSS with Reduced Communication Complexity," CT-RSA 2013, San Francisco, Feb 2013
- ◇ "ObliviAd: Provably Secure and Practical Online Behavioral Advertising," IEEE Symposium on Security and Privacy 2012, San Francisco, May 2012.

- ◇ "Adding query privacy to robust DHTs," AsiaCCS 2012, Seoul, May 2012.
- ◇ "On the (limited) power of non-equivocation," ACM PODC 2012, Mallorca, July 2012.
- ◇ "Constant-Size Commitments to Polynomials and Their Applications," ASIACRYPT 2010, Signapore, Dec 2010.
- ◇ "Using Sphinx to Improve Onion Routing Circuit Construction," Financial Cryptography 2010, Tenerife, Feb 2010.
- ◇ "Distributed Private-Key Generators for Identity-Based Cryptography," SCN 2010, Amalfi, Sep 2010.
- ◇ "Distributed Key Generation for the Internet," ICDCS 2009, Toronto, June 2009.
- ◇ "Anonymity and security in delay tolerant networks," SecureComm 2007, Nice, September 2007.
- ◇ "Pairing-Based Onion Routing," Privacy Enhancing Technologies 2007, Ottawa, July 2007 .
- ◇ Talks and posters at workshops/events held at or by Purdue University, 2015-2019 (Selected):
  1. "Optimized Distributed Analytics for Dynamic CPS and IoT: Removing the Need for a Centralized Aggregator" 22nd Annual CERIAS Security Symposium, Purdue University, September 2020.
  2. "GDPR Privacy vs. Blockchain Transparency – Is it really technology against the law?" 21st Annual CERIAS Security Symposium, Purdue University, April 2019.
  3. "A Technical Perspective on the Future of Decentralization" 20th Annual CERIAS Security Symposium, Purdue University, April 2018.
  4. "Blockchains and Crypto Currencies From Hype to Reality Dawn or Doom" at Dawn-or-Doom 2017 Conference, Purdue University. Sep 2017

Software Systems Developed

- ◇ "Distributed Key Generation (DKG) for use over the Internet", URL: `https://crysp.uwaterloo.ca/software/DKG/`.
  The DKG library is a multi-threaded C++ implementation associated with [55, 74]. It is employed and formed the basis of distributed key generation instantiations for distributed systems startups such as Helium, PoANetworks, and Tor.us.
- ◇ "Check Your Secondary Digital Footprint on Twitter!", URL: `https://twitter-app.mpi-sws.org/footprint/`.
  This is an education and informative Twitter app associated with [32] This app aims educating users about their secondary digital footprints on systems such as Twitter and their risks.
- ◇ "DiceMix P2P mixing", URL: `https://github.com/ElementsProject/dicemix`.
  This library is associated with [29]. The library employed by privacy-preserving blockchains such as ElementsProject and Decred.

Research Grants and Proposals

Funded Projects

- ◇ MITRE/Practical Secure Computation
  (CO-PI) 33% of $150,000 10/01/20 - 09/30/21
- ◇ ARL/Consensus under Energy Constraints for Dynamic Distributed Cyber-Physical Systems
  (CO-PI) 35% of $831,974 10/01/19 - 09/30/22
- ◇ IARPA/HACCLE: High-Assurance Compositional Cryptography: Languages and Environments
  (CO-PI) 9% of $1,700,000 06/01/19 - 06/31/20
- ◇ NSF/CAREER: Towards Privacy and Availability of Inter- blockchain Communication
  (PI) 100% of $429,983 02/06/19 - 01/31/24
- ◇ Tor.us labs/Unrestricted Gifts
  (PI) 100% of $30,000 02/01/19 - open ended
- ◇ Keyless Inc/Unrestricted Gifts
  (PI) 100% of $27,500 11/15/18 - open ended

- ◇ Deuro/Unrestricted Gifts
  (PI) 100% of $40,000 08/01/18 - open ended
- ◇ Ford-Purdue Alliance/Supply Chain Transparency and Control using Blockchain Technology
  (PI) 100% of $278,031 09/01/17 - 10/31/19
- ◇ NSF/SaTC-BSF: CORE: Small: Collaborative: Making Blockchains Scale Privately and Reliably
  (PI) 50% of $512,302 08/17/17 - 12/31/20
- ◇ NGCRC/DUST-BT: Detection of Unauthorized Supply Chain Tampering using Blockchain Technology
  (Co-PI) 100% of $226,579 09/01/16 - 08/31/18
- ◇ NSF/TWC: Small: Practical Assured Big Data Analysis in the Cloud
  (PI) 100% of $439,000 01/01/17 - 08/31/19

INTERNAL FUNDING

- ◇ CERIAS Seed Grant/ Reinventing Blockchain Technology for Secure Provenance in Large-Scale CPS
  (PI) 50% of $45,000 08/20/18 - 10/31/19
- ◇ PRF/Understanding Fundamental Constraints for Anonymous Communication
  (PI) 100% of $25,000 (1 graduate student 100% of total) 08/20/18 - 08/14/19
- ◇ PRF/Systematic Testing of Certificate Chain Validation Logic
  (CO-PI) 50% of $25,000 (1 graduate student 100% of total) 08/20/16 - 08/14/17

PROPOSALS IN SUBMISSION

I have four pending proposals / in-negotiation projects with DOE (1), Ford Motors (1) and NSF (2) as of October 2020.

GRADUATED STUDENTS

GRADUATED PHD STUDENTS

- ◇ Mohsen Minaei, Purdue University, Fall 2015–Summer 2020.
  Thesis Title: Privacy Preserving Systems with Crowd Blending
  Last known Employment: Visa Research
- ◇ Sze Yiu Chau (co-advised with Ninghui Li), Fall 2015–Summer 2019.
  Thesis title: Systematic Evaluation of Security Mechanism Deployments.
  Last known Employment: Assistant Professor, Chinese University of Hong Kong (CUHK)
- ◇ Tim Ruffing, Saarland University (co-advised with Dominique Schroeder as I left Saarland), Spring 2013–Summer 2019.
  Thesis title: Cryptography for Bitcoin and Friends.
  Last known Employment: Blockstream
- ◇ Pedro Moreno-Sanchez, Purdue University, Fall 2013–Summer 2018.
  Thesis title: Credit Network Payment Systems: Security, Privacy and Decentralization.
  Last known Employment: Assistant Professor, IMDEA Software Institute, Madrid

GRADUATED MASTER THESIS STUDENTS

- ◇ Siddharth Gupta at Interdisciplinary Graduate Program in Information Security, CERIAS, 2016–2017.
  Thesis title: Burning Bitcoins for Censorship Resistance.
- ◇ Simon Heinzel at Saarland University, Germany, 2015–2016.
  Thesis title: Novel distributed trusted-party time-release encryption protocol.
- ◇ Tobias Theobald at Saarland University, Germany, 2015–2016.
  Thesis title: Identity Web of Trust.
- ◇ Uzair Mahmood at Saarland University, Germany, 2014–2015.
  Thesis title: Ensuring integrity of recommendations in a Marketplace.
- ◇ Ivan Pryvalov at Saarland University, Germany, 2013–2014.
  Thesis title: Introducing Fault Tolerance into Threshold Password-Authenticated Key Exchange.

CURRENT STUDENTS

- ◇ Debajyoti Das, Ph.D. Student in Computer Sciences, Research Assistant.
  Dissertation topic: Foundations for Anonymous Communication. (Prelim Exam Completed; graduating in 2021).
- ◇ Duc V Le, Ph.D. Student in Computer Sciences (co-adviser: Mikhail Atallah), Research Assistant.
  Dissertation topic: Cryptographic Systems with Flexible Security. (Prelim Exam Scheduled; graduating in 2021).
- ◇ Easwar V Mangipudi, Ph.D. Student in Computer Sciences, Research Assistant.
  Dissertation topic: Accountable Threshold Cryptography. (Plan of Study approved; graduating in 2021).
- ◇ Donghang Lu, Ph.D. Student in Computer Sciences, Research Assistant.
  Dissertation topic: Anonymous Distributed Computing. (Plan of Study approved; graduating in 2022).
- ◇ Adithya Bhat , Ph.D. Student in Computer Sciences, Research Assistant.
  Dissertation topic: Consensus and MPC for CPS. (Plan of Study in progress graduating in 2023).
- ◇ Albert Yu, Ph.D. Student in Computer Sciences, (co-adviser: Hemanta Maji) Research Assistant.
  Dissertation topic: Multi-party Computation. (Plan of Study in progress graduating in 2024).
- ◇ Tiantian Gong, Masters. Student in Computer Sciences, Research Assistant.
  Dissertation topic: Game Theoretic Cryptography. (Plan of Study in progress graduating in 2024).

UNDERGRADUATE STUDENTS

- ◇ Shivam Bajpai (supported by Purdue SURF program and grant money), 2018–*2019*.
  (Resulted Publication: [61])
- ◇ Sihao Yin (supported by Purdue's Summer Stay Scholar and grant money), 2018–2019.
  (Resulted Publication: [61])
- ◇ Lizzy Tengana Hurtado (supported by Purdue's UREP-Columbia program and grant money) , 2018.
  (Resulted Publication: [3])
- ◇ Krutarth R. Rao (supported by Summer Stay Scholar and grant money), 2016–2018
  (Resulted Publication: [60])(**Received outstanding Undergraduate Research Award, CS, Purdue, 2018)**
- ◇ Mahimna Kelkar (supported by NSF REU), 2016–2018.
  (Resulted Publication: [18])
- ◇ Durga Keerthi Mandarapu (from IIT–Hyderabad) (supported by Purdue-CS GoBoiler program), 2018.
- ◇ Joy Wen (from U. Waterloo) (supported by Purdue-CS GoBoiler program), 2017.
- ◇ Rachit Garg (from IIT-Madras) (supported by Purdue Undergraduate Research Experience (PURE) program), 2016
- ◇ Niklas Grimm (Bachelor Thesis at Saarland University), 2012–2013.
  (Resulted Publication: [9, 63])

SERVICE ON MS/PHD COMMITTEES

QUAL II COMMITTEE MEMBERSHIPS

Savvas Savvides (2016)
Huangyi Ge (2016)
Xin Cheng (2016)
Lina Alfantoukh (IUPUI, 2015)
Pedro Moreno-Sanchez (@Saarland University, 2015)
Praveen Manoharan (@Saarland University, 2014)
Ivan Pryvalov (@Saarland University, 2014)
Tim Ruffing (@Saarland University, 2014)
Malte Skoruppa (@Saarland University, 2013)
Sven Bugiel (@Saarland University, 2013)
Milivoj Simeonovski (@Saarland University, 2013)

Preliminary Exam/Final Committee Memberships

Manish Nagaraj (Masters Final, ECE, Purdue University, 2019)
James Lembke (PhD Prelim, 2019)
Udyani Herath Mudiyanselage (PhD Final, QUT, Australia, 2018-19)
Javad Darivandpour (PhD Prelim, 2018)
Manuel Reinert (PhD Final, Saarland University, 2018)
Yonghwi Kwon (PhD Prelim+Final, 2017-18)
Julian Stephen (PhD Prelim+Final, 2016-17, Departmental Advisor in absence of P. Eugster)
Brendan Saltaformaggio (PhD Prelim+Final, 2016)
Yefeng Ruan (PhD Prelim+Final, IUPUI, 2016)
Sebastian Meiser (PhD Final, Saarland University, 2016)
Scott Carr (PhD Prelim+Final, 2015-17)

Other Mentoring

Graduate Students

Akhil Bandarupalli, Research Advisor, Fall 2020.
Rumela Ghosh, Research Advisor, Summer/Fall 2020.
Sri Yogesh Dorbala, Research Advisor, (CS 590), Fall 2017.
Miguel Villarreal-Vasquez, Research Advisor, (CS 699, Fall 2015).
Satrajit Ghosh, Research Advisor, (at Saarland University, 2014).
(Resulted Publication: [35])
Aastha Mehta, Research Advisor, (at Saarland University, 2014).
Muhammad Bilal Zafar, Research Advisor, (at Saarland University, 2014)
(Resulted Publication: [8 ,33])

Teaching Experience

Teaching Assignments

Purdue University

(CS 426) Computer Security (3 credits, 58 students)	Fall 2020
(CS 59100 - RS1) Res Sem First Yr Gr Student (1 credit, 41 students)	Fall 2020
(CS 590-BTS) Blockchains & Cryptocurrencies (3 credits, 05 students)	Spring 2020
(CS 426) Computer Security (3 credits, 58 students)	Fall 2019
(CS 528) Network Security (3 credits, 21 students)	Spring 2019
(CS 590-BTS) Blockchains & Cryptocurrencies (**New course**, 3 credits, 14 students)	Spring 2019
(CS 528) Network Security (3 credits, 27 students)	Spring 2018
(CS 426) Computer Security (3 credits, 44 students)	Fall 2017
(CS 591) CERIAS Security Seminar (1 credit, 18 students)	Spring 2017
(CS 528) Network Security (Reworked, 3 credits, 06 students)	Spring 2017
(CS 426) Computer Security (Significantly redesigned, 3 credits, 41 students)	Fall 2016
(CS 528) Network Security (**New course**, 3 credits, 13 students)	Spring 2016
(CS 690-PET) Hot Topics in Privacy Enhancing Technologies (3 credits, 07 students+audits)	Fall 2015

Saarland University

Advanced Course: Applied Cryptography	Winter 2014/15
Seminar: Practical Cryptographic Systems	Winter 2012/13, Summer 2014
Advanced Course: Privacy Enhancing Technologies (co-taught)	Summer 2013, 2014, 2015

Other Contributions to Undergraduate Education

- *Seminar Talk on Cryptography, CS 197 Freshman Honors Seminar. Spring 2017, 2018.*
- *Seminar Talk on Computer Security and Privacy Research, CS 397 Honors Seminar. Fall 2015-16, 2019.*
- *Invited Lecture on for Global Science Leadership Seminar (SCI 19500), Fall 2018.*
- *Invited Talk on Blockchains, BoilerMake Hackathon 2017. September 2017.*

- *Introducing Research to Undergraduate. Summer 2016–present*
  09 undergraduate students (06 from Purdue and 03 from outside)
  CS39000: Individual Study courses, undergraduate research assistants and NSF REU

ENGAGEMENT AND SERVICE

DEPARTMENTAL ENGAGEMENT

- Started the Crypto Reading Group, (weekly meetings), Attendance: 20 graduate students and faculty members, Spring 2016–*present*
- Committees
  - Member of the Graduate Admissions committee, 2015–2018, Purdue University.
  - Member of the Security Faculty Search committee, 2018–2019, Purdue University.
  - Member of the Graduate Student Board Advisor committee, 2018–2020, Purdue University.
  - Member of the Graduate Study committee, 2019–2020, Purdue University.
  - Member of the Colloquia committee, 2019–2020, Purdue University.
  - Member of the Awards committee, 2020–2021, Purdue University.
- Presentation for engagement seminars
  - CS 591: Research Seminar for Graduate Students, 2017, 2018, 2019.
  - Corporate Partner Meeting: Fall 2017.

COLLEGE-LEVEL ENGAGEMENT

- Offered a lecture as part of Global Science Leadership Seminar, College of Science, Fall 2018.

UNIVERSITY-LEVEL ENGAGEMENT

- Organizing Committee Member for the "Big Data, Safe Food" Conference, 2020 (Delayed due to Pandemic)
- Started the Blockchain Research meetings, (weekly meetings). Attendance: 15 graduate/undergraduate students across the campus, Fall 2016–*present*
- Security Applications (IE 590): Purdue Online Learning (1 lecture on Blockchain Applications), Fall 2018
- the ONR STEM course (1 lecture on Cyber Security every year), 2017-18. Also helped preparing to the online version of the course: CNIT 581
- Industry Engagement Talk for CERIAS and Purdue University' Office of Corporate & Global Partnerships: Monsanto (2018), Master Card (2018), ARL (2018), Raytheon (2018), KAR (2018), SRC (2018), John Deere (2017), Intel (2017).
- Member, Interdisciplinary Graduate Program in Information Security (INSC) Admission Committee, CERIAS, Purdue University, 2016
- Introduction to blockchains, Research Seminar Series, School of Industrial Engineering, September 2017

PROFESSIONAL SERVICE

- Editorial Board: Proceedings on Privacy Enhancing Technologies (PoPETS) 2018-2019
- Track Chair on Blockchain, IEEE Computer Security Foundations (CSF) 2019
- Technical Program Area Chair, IEEE Conference on Communications and Network Security (CNS) 2019
- Poster/Demo co-Chair, ACM Computer and Communication Security (CCS) 2016
- Proceedings co-Chair, ACM Computer and Communication Security (CCS) 2018
- Selected Program Committee Membership:
  [at Purdue]
  IEEE Symposium on Security and Privacy 2019-21.
  World Wide Web Conference (WWW) 2021.
  Usenix Security Symposium 2018, 2020.
  Financial Cryptography and Data Security (FC) 2016, 2019-21.

ACM Computer and Communication Security (CCS) 2017-19.
Network and Distributed System Security Symposium (NDSS) 2018-19.
The Web Conference (WWW) 2019, 2021.
IEEE Computer Security Foundations (CSF) 2017, 2019.
International Conference on Privacy, Security and Trust (PST) 2017.
Principles of Security and Trust (POST) 2017.
Advances in Cryptology—Eurocrypt 2016.
IEEE International Conference on Distributed Computing Systems (ICDCS) 2016-18.
The Bitcoin Workshop 2016-18.
International Conference on Applied Cryptography and Network Security (ACNS) 2016-18.
ACM Cloud Computing Security Workshop (CCSW) 2015.
ACM Workshop on Privacy in the Electronic Society (WPES) 2015, 2017, 2018, 2020.
[before Purdue]
IEEE International Conference on Distributed Computing Systems (ICDCS) 2015.
ACM Cyber-Physical System Security Workshop (CPSS) 2015.
IEEE International Conference on Cloud Computing Technology and Science (CloudCom) 2015.
Workshop on Foundations of Computer Security (FCS) 2015.
Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs) 2014.
International Conference on Provable Security (ProvSec). 2014-15.
World Wide Web Conference (WWW) 2013.
ACM Workshop on Privacy in the Electronic Society (WPES) 2012.

- ◇ NSF SaTC Panelist (In-person / Virtual, One panel/year), 2016-18
- ◇ NSF External Reviewer (multiple/year), 2018-20
- ◇ Industrial Advisor: Deuro, Keyless, Torus, 2018-*present*

DIVERSITY ACTIVITIES

- ◇ Invited Talk, Black Graduate Student Association, Purdue University, February 2018 (Attended by more than 20 students from diverse international background)
- ◇ Hosted female students
  - · Lizzy Tengana Hurtado from Columbia as part of Purdue's UREP-C program, 2018
  - · Durga Keerthi Mandarapu from India as part of the GoBoiler internship program, 2018 joined our Ph.D. program in Fall 2019
  - · Jing Wen from China, 2017
  - · Christiane Kuhn from Germany, 2019

OTHER ACTIVITIES

- ◇ Research Group Leaders' Representative at Cluster of Excellence Board, Saarland University, 2013-15.
- ◇ Graduate Students' Representative at Director Search Committee, School of Computer Science, University of Waterloo, 2009-10.
- ◇ Cryptography Seminar Organizer for the Centre for Applied Cryptographic Research (CACR), University of Waterloo, Spring 2008.
- ◇ Overall Coordinator for Annual Network Security (SecNet 2006) Workshop, IIT-Bombay, Spring 2006